



CS 598: Spectral Graph Theory. Lecture 10

PRGs and Random Walks
on Expanders

Alexandra Kolla

Today

- Why PRGs?
- The use of PRGs in randomized algorithms
- Introduce expander graphs
- Random walks on expanders and Impagliazzo-Zuckerman PRG

Why Study PRGs?

- Pseudo-random number generators take a seed which is presumably random and generate a long string of random bits that are supposed to act random.
- Why would we want a PRG?
 - Random bits are scarce (eg low-order bits of temperature of the processor in computer is random, but not too many such random bits). Randomized algorithms often need many random bits.
 - Re-run an algorithm for debugging, convenient to use same set of random bits. Can only do that by re-running the PRG with the same seed, but not with truly random bits.

What Type of PRGs?

- Standard PRGs are terrible (e.g. rand in C). Often produce bits that behave much differently than truly random bits.
- One can use cryptography to produce such bits, but much slower

Repeating an Experiment

- Consider wanting to run the same randomized algorithm many times.
- Let A be the algorithm, which returns "yes"/"no" and is correct 99% of the time (correctness function of the random bits)
- Boost accuracy by running A t times and taking majority vote
- Use truly random bits the first time we run A and then with the PRG we will see that every new time we only need 9 random bits.
- If we run t times, probability that majority answer is wrong is exponential in t .

The Random Walk Generator

- Let r be the number of bits out algorithm needs for each run: space of random bits is $\{0,1\}^r$
- Let $X \subseteq \{0,1\}^r$ be the settings of random bits on which algorithm gives wrong answer
- Let $Y = \{0,1\}^r \setminus X$ be the settings on which algorithm gives the correct answer

The Random Walk Generator: Expander Graphs

- Our PRG will use a random walk on a d -regular G with vertex set $\{0,1\}^r$, and degree $d = \text{constant}$.
- We want G to be an expander in the following sense: If A_G is G 's adjacency matrix and $d = \alpha_1 > \alpha_2 \geq \dots \geq \alpha_n$ its eigenvalues then we require that

$$\frac{|\alpha_i|}{d} \leq \frac{1}{10}$$

Such graphs exist with $d=400$ (next week)

The Random Walk Generator

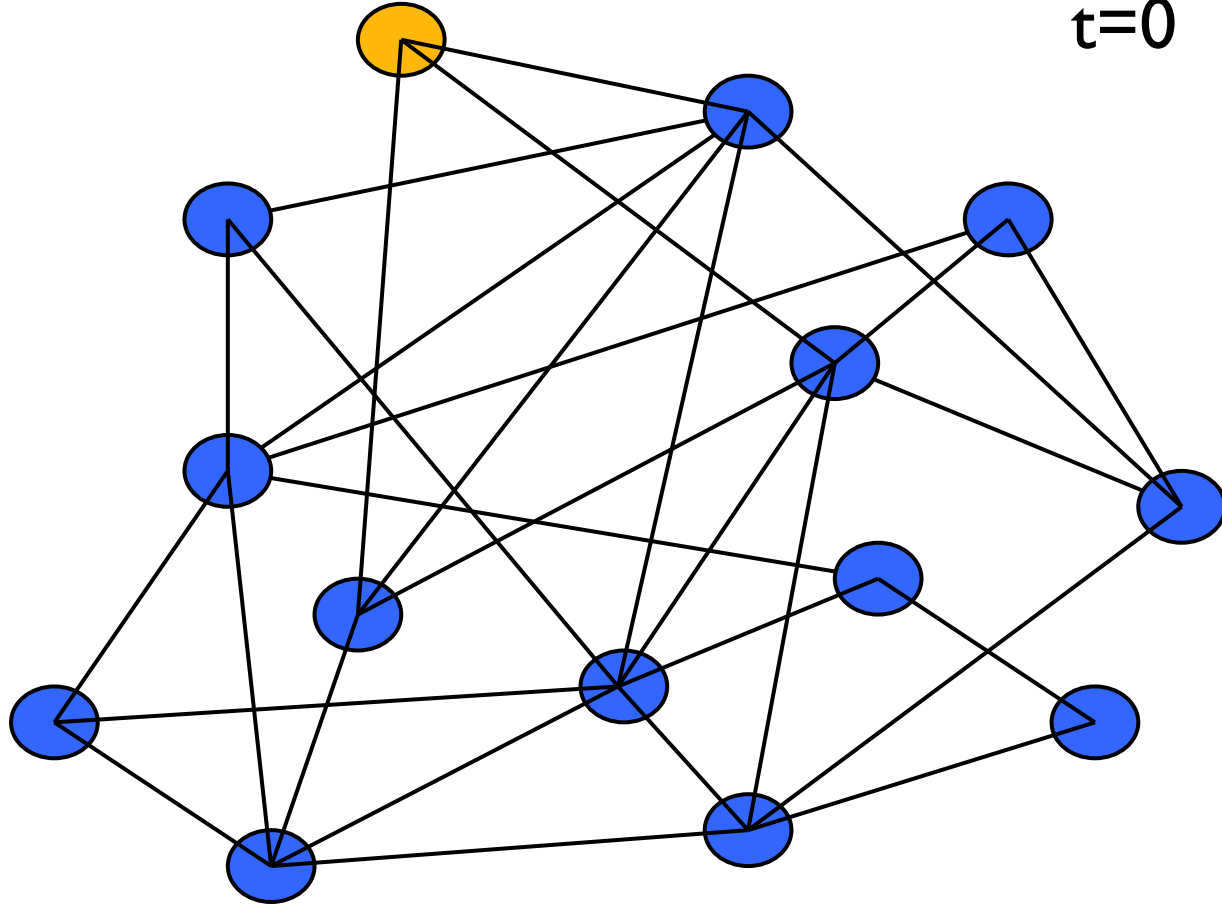
- For the first run of algorithm, we require r truly random bits. Treat those bits as vertex of expander G .
- For each successive run, we choose a random neighbor of the present vertex and feed the corresponding bits to our algorithm.
- I.e, choose random i between 1 and 400 and move to the i -th neighbor of present vertex. Need $\log(400) \sim 9$ random bits.
- Need concise description, don't want to store the whole graph (e.g. see hypercube)

The Random Walk Generator

G

$$v_0 \in \{0,1\}^r$$

t=0

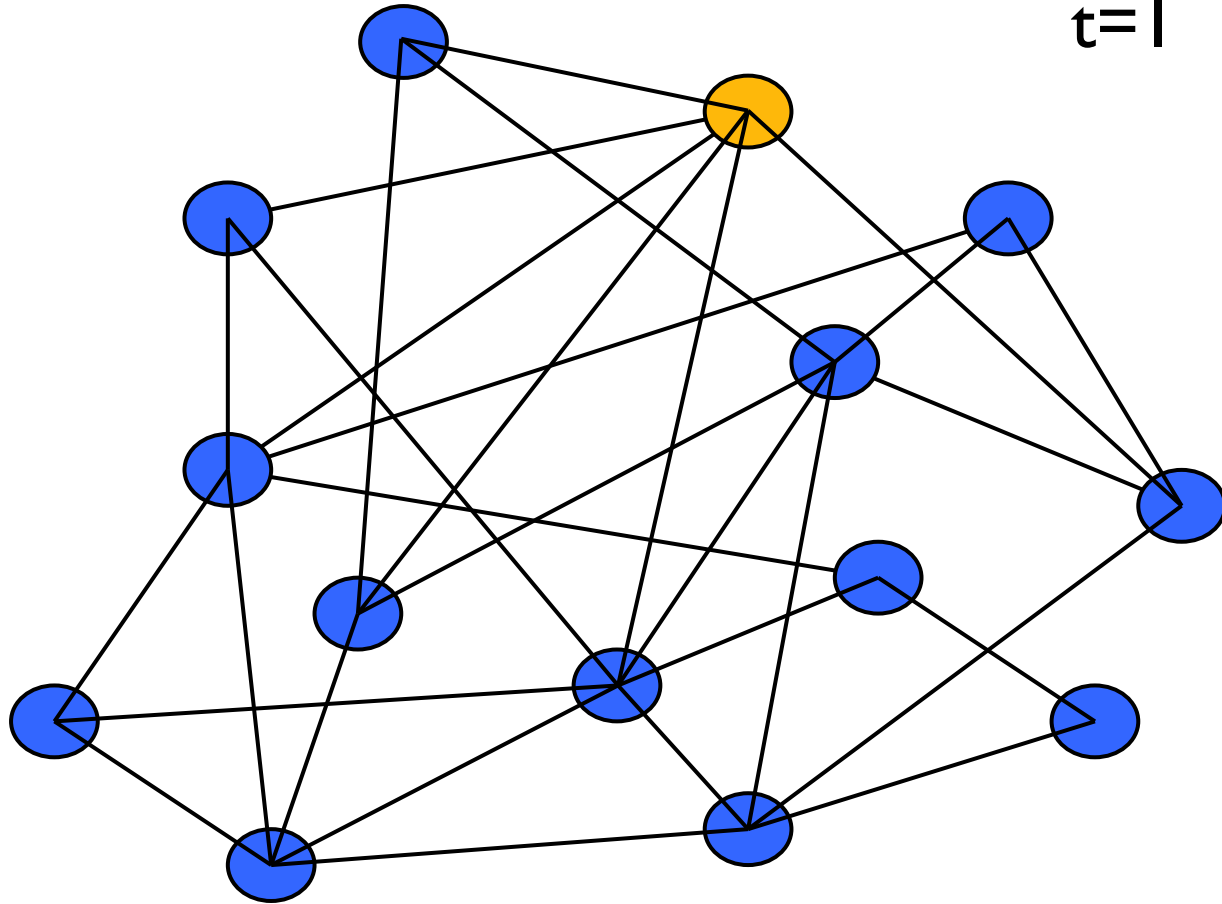


The Random Walk Generator

G

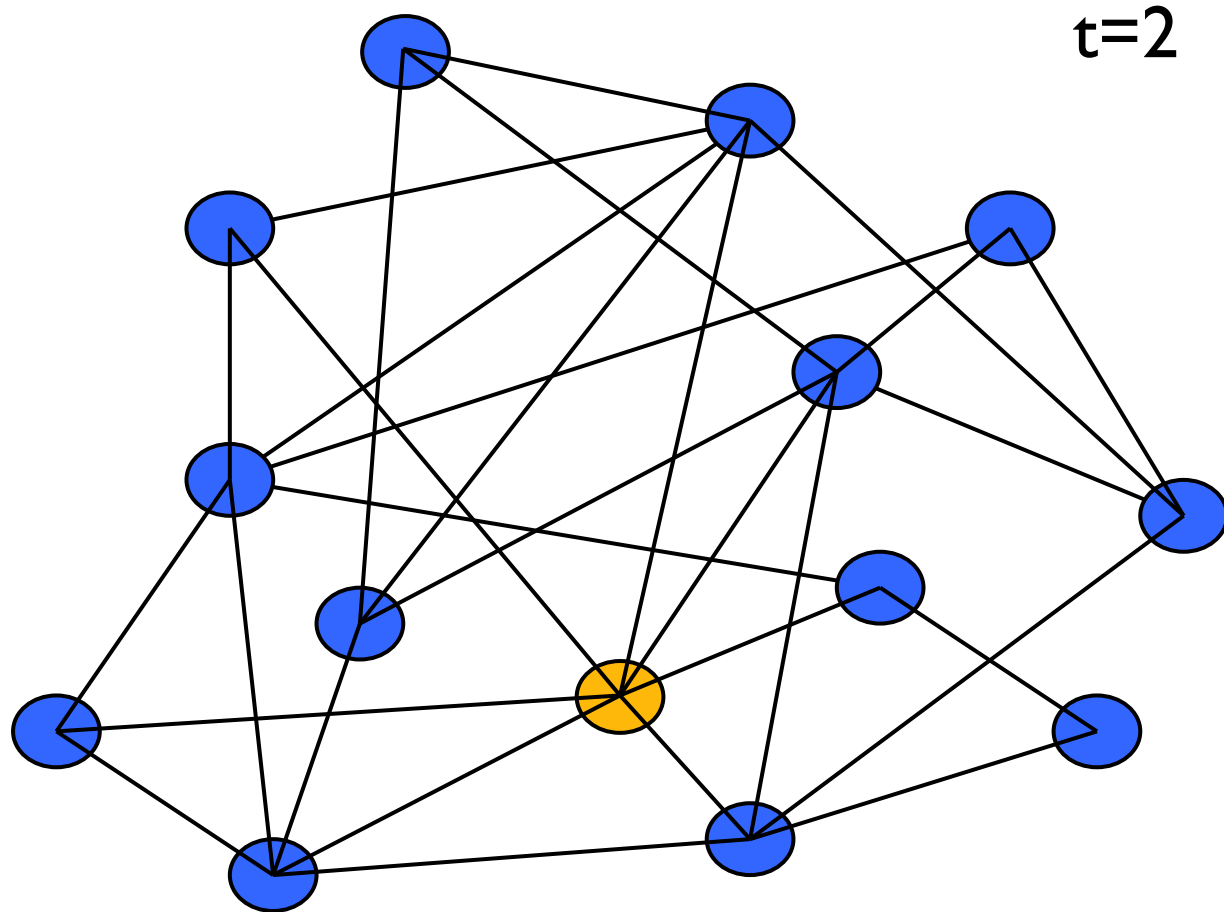
$$v_1 \in N(v_0)$$

t=1



The Random Walk Generator

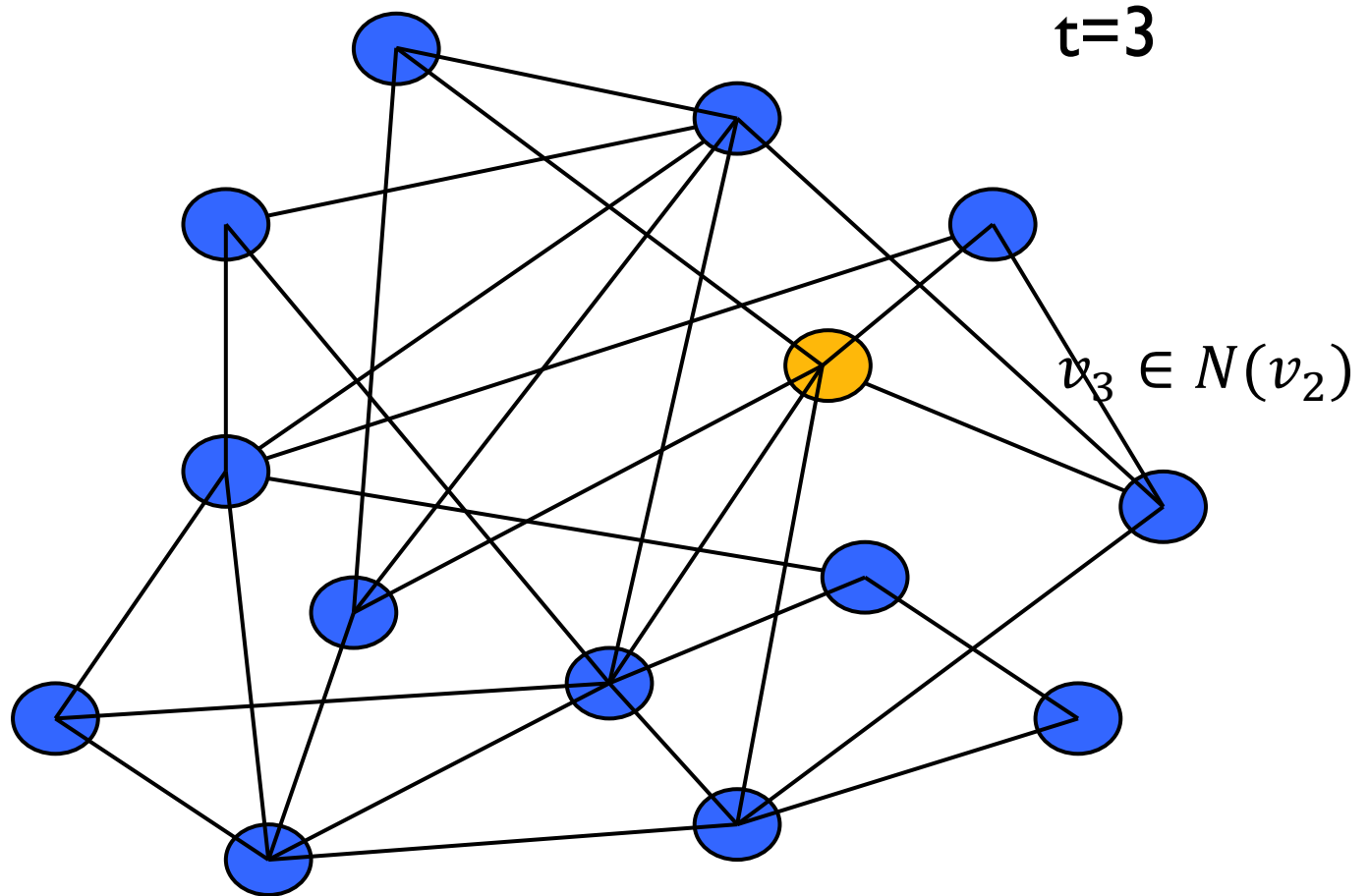
G



$$v_2 \in N(v_1)$$

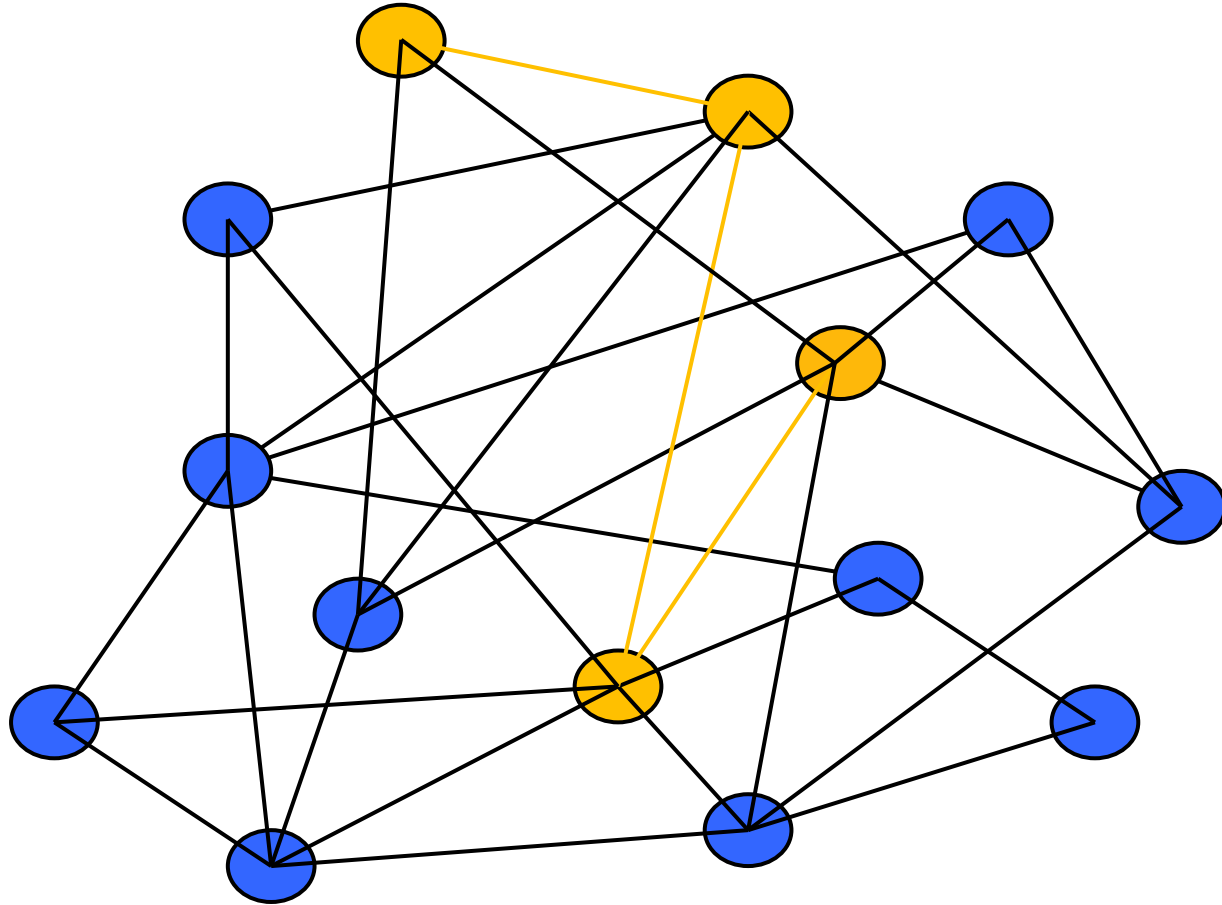
The Random Walk Generator

G



The Random Walk Generator

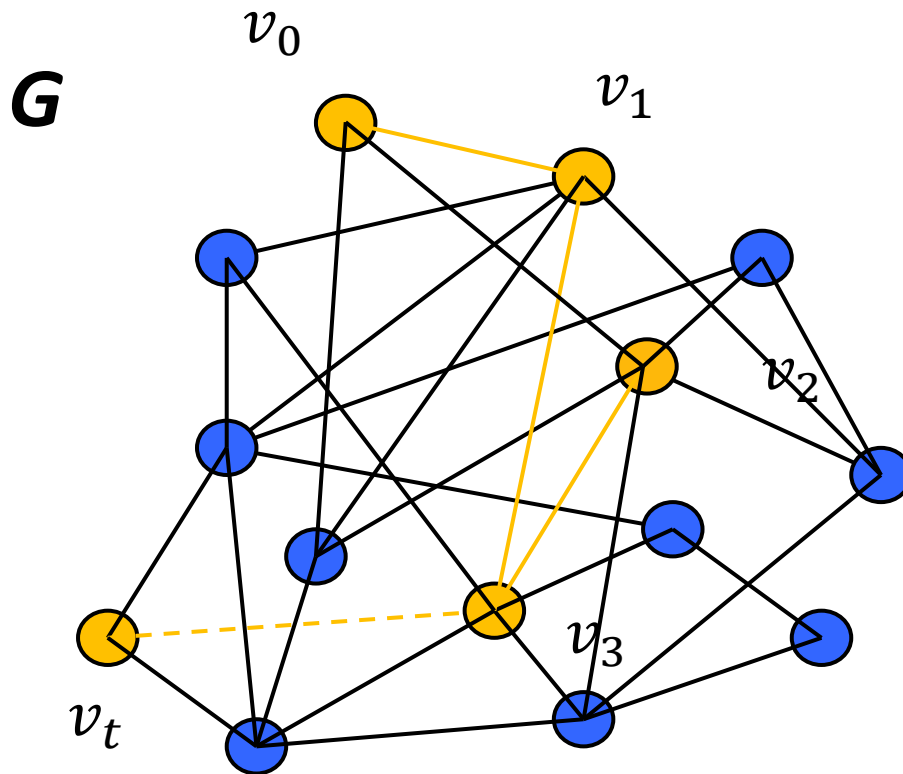
G



Formalizing the Problem

- Assume we will run the algorithm $t+1$ times. Start with truly random vertex u and take t random walk steps.
- Recall that X is the set of vertices on which the algorithm is not correct, we assume that $|X| \leq \frac{2^r}{100}$ (algorithm correct 99% of time)
- If at the end, we report the majority of the $t+1$ runs of algorithm, then we will return the correct answer as long as the random walk is inside X less than half the time.

The Random Walk Generator



$T = \{0, \dots, t\}$ time steps

$S = \{i : v_i \in X\}$

We will show that

$$\Pr[|S| > t/2] \leq \left(\frac{2}{\sqrt{5}}\right)^{t+1}$$

Formalizing the Problem

- Initial distribution is uniform (start with truly random string): $\mathbf{p}_0 = \mathbf{1}/n$
- Let χ_X and χ_Y the characteristic vectors of X and Y .
- Let $D_X = \text{diag}(X)$ and $D_Y = \text{diag}(Y)$
- Let $W = \frac{1}{d}A$ (not lazy) random walk matrix, with eigenvalues $\omega_1, \dots, \omega_n$ such that $\omega_i \leq \frac{1}{10}$ by the expansion requirement.
- For $|X| \leq \frac{2^r}{100}$,
 $S = \{i: v_i \in X\}$ (time steps that the walk is in X)
we want to show $\Pr[|S| > t/2] \leq \left(\frac{2}{\sqrt{5}}\right)^{t+1}$